UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,523	02/27/2004	Atsushi Minemura	NGB-36483	6891

116 7590 07/09/2008

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/788,523	MINEMURA, ATSUSHI	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/08/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on April 09, 2008.

2. Claims 2-5 and 8-13 are amended; and Claims 1 and 7 are previously presented.

3. **Claims 1-13** are pending.

Response to Arguments

4. Applicant's arguments filed on 04/09/2008 have been fully considered but they are not persuasive.

Regarding 35 U.S.C. 112, second paragraph Rejection

Applicant argued: "*...the terms 'no secure information concealing area' are discernable and are not insolubly ambiguous and, therefore, are not indefinite... one of ordinary skill in the art would readily understand the term 'information' to be synonymous with data, and 'concealing area' to mean a memory location for concealing the data.*'

Examiner respectfully disagrees. Based on Applicant's argument [and explanation], the claim term "***no secure information concealing area***" would be defined as "***no secure memory location for concealing the data***". However, this definition still does not make the claim term clear. Applicant is reminded that the specification of the invention discloses the terminal device with '***writable***' and '***un-writable***' areas [areas 301 & 302 of device 30 in FIGS.1-6], but does not disclose the claimed terminal device with '***no secure information concealing area***' or '***no secure memory location for concealing the data***' or '***lack of memory location for concealing secure data***'. Therefore, the 112 2nd paragraph rejection made on the prior office action is not withdrawn.

Prior Art Rejection

Regarding Claim 1, 7, 8 and 11 - Applicant argued: *"...Applicant submits that the cited combination of references fails to teach, or otherwise render foreseeable, a terminal device having no secure information concealing area, as required by claim 1, and that claim 1 is allowable over the cited combination of references"*

Examiner respectfully disagrees. As discussed above, the claim term **'no secure information concealing area'** is still considered unclear and indefinite. Thus, Applicant's argument the cited references not teaching **'no secure information concealing area'** is not persuasive.

Regarding Claim 12 and 13 – Applicant argued: *"...The cited combination of references does not teach an application execution runtime environment that executes an application and which is verified and invoked by a separate operating system..."*

Examiner respectfully disagrees. As indicated in the prior office action, DeTreville discloses a terminal device [**Computer 118**] which has an application execution runtime environment [see FIG.11 and **CPU 134** in FIG.3, for example] and an operating system [see **Operating System** in FIGS.2 and 3], which is placed in the **Nonvolatile Memory 136** [which is separate from CPU 134].

5. Applicant's arguments with respect to the amended claims **[3** and **4]** have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 7, 8 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 7, 8 and 11 recite "*a terminal device having no secure information concealing area* ..." The detailed description of the invention mentions the underlined term [on page 4, lines 23-24; page 5, lines 4-5, page 6, lines 9-10; page 14, lines 19-20; and page 23, lines 10-11]; however, the specification does not define what the "*no secure information concealing area*" is. Additionally, the specification of the invention discloses the terminal device with '***writable***' and '***un-writable***' areas [areas 301 & 302 of device 30 in FIGS.1-6], but does not disclose the claimed terminal device with '***no secure information concealing area***' or '***no secure memory location for concealing the data***' or '***lack of memory location for concealing secure data***'.

Therefore, the claimed invention is rendered indefinite for being unclear.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2 and 5-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeTreville et al. (US 6,609,199 B1, referred as "DeTreville") in view of "Barlow" (US 6,484,259 B1)

As per Claim 1, DeTreville teaches,

An application authentication system comprising: a terminal device having no secure information concealing area [see **Computer 118** in FIGS.1 and 2], said terminal device including an application [see **Applications 124** and **S/W Program(s)** in FIGS.2, 3 and 11] and application running means [see **Operating System 123-160** in FIGS.2, 3 and 11; and for example, col.4, line 64 to col.5, line 34]; and

said secure device for authenticating the application requesting access to the secure device [see for example, col.3, line 62 to col.5, line 34];

wherein said secure device authenticates the application running means [see abstract; and for example, col.2, line 33 to col.3, line 5], and then authenticates the application based on a result of a process that the application running means executes on the application [see FIGS.13-15; and for example, col.21, line 65 to col.26, line 3].

DeTreville teaches a secure device connected detachably to said terminal device [see **Portable Device 116** in FIGS.1 and 2]; but fails to teach a secure device connected fixedly. However, in the same field of endeavor, Barlow teaches a secure device connected fixedly [see **SC-CPS 246** in FIG.3; abstract; and for example, col.8, lines 2-39].

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention was made, to attach the secure device fixedly to the terminal in order to implement a fast and easily accessible static security system [see col.1, line 20 to col.3, line 15 of **Barlow**].

As per Claim 7, DeTreville teaches,

A secure device **[IC Device]** connected detachably to a terminal device [see **116** in FIGS.1 and 2; and for example, col.4], said secure device comprising: a card manager for executing a process of authenticating the terminal device; and a card application for applying an authenticating process to an access request application stored in the terminal device [see **Processor 128** and **Authentication Application 130** in FIG.2; see for example, col.4, line 64 to col.5, line 34];

wherein the terminal device has no secure information concealing area [see **Computer 118** in FIGS.1 and 2], and

wherein the card application authenticates the application based on a process that is applied to the application by the terminal device [see abstract; and for example, col.2, line 33 to col.3, line 5], then confirms that the process of authenticating the terminal by the card manager is completed, and then accepts an access request of the authenticated application [see FIGS.13-15; and for example, col.21, line 65 to col.26, line 3].

Barlow discloses secure device connected fixedly [see **SC-CPS 246** in FIG.3; abstract; and for example, col.8, lines 2-39]. It would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention was made, to attach the secure device fixedly to the terminal in order to implement a fast and easily accessible static security system [see col.1, line 20 to col.3, line 15 of **Barlow**].

As per Claim 8, DeTreville-Barlow combination teaches,

A terminal device [**Computer 118**] including: an application execution runtime environment [see **CPU 134** in FIG.3];

an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking the application execution runtime environment [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7]; and

an application stored in the terminal device [see **Applications 124** and **S/W Program(s)** in FIGS.2, 3 and 11] and executed by the application execution runtime environment [see FIGS.2 and 3 – *where DeTreville discloses executing applications in the runtime environment of Computer 118*. See also FIG.11 – *where runtime environment disclosed*],

wherein the terminal device has no secure information concealing area [see **Computer 118** in FIGS.1 and 2], and

wherein the application execution runtime environment calculates digest data of the application to request an access to a fitted secure device [see **SC-CPS 246** in FIG.3; abstract; and for example, col.8, lines 2-39 of **Barlow**] after the fitted secure device authenticates the application execution runtime environment [see FIGS.13-15; and for example, col.21, line 65 to col.26, line 3], then authenticates the application by using the digest data, and then issues an access request to the secure device [see FIGS.1-6; and for example, col.3, line 60 col.11, line 12].

As per Claim 11, DeTreville-Barlow combination teaches,

An application authentication system comprising: a terminal device having no secure information concealing area [see **Computer 118** in FIGS.1 and 2]; and

a secure device connected fixedly or detachably to said terminal device [see **Portable Device 116** in FIGS.1 and 2. See also **SC-CPS 246** in FIG.3; abstract; and for example, col.8, lines 2-39 of **Barlow**];

wherein said terminal device includes applications [see **Applications 124** and **S/W Program(s)** in FIGS.2, 3 and 11], an application execution runtime environment for running and authenticating the applications requesting access to the secure device [see FIGS.2, 3 and 11], and an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking the application execution runtime environment [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7]; and

wherein said secure device authenticates an application stored in the terminal device in order to permit access to said secure device [see abstract; and for example, col.2, line 33 to col.3, line 5], if the application is authenticated by application execution runtime environment, which is authenticated by said secure device [see FIGS.13-15; and for example, col.21, line 65 to col.26, line 3], and

wherein the application execution runtime environment calculates digest data of said application and verifies an electronic signature attached to the application by using the digest data, and authenticates the application [see FIGS.1-6; and for example, col.3, line 60 col.11, line 12].

As per Claim 2, DeTreville-Barlow combination teaches,

an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking said application running means [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7], wherein said application running means is an application execution runtime environment [see FIGS.2, 3 and 11],

wherein an application electronic signature that certifies a validity of the application is attached to the application [see **Signed Boot Block 180,** containing **Signature 186** in FIG.4],

wherein the application running means calculates digest data of the application to which the application electronic signature is attached [see **Operating System 160, Boot Log 158 and Boot Block**

162 in FIG.3. See also **Signed Boot Block 180** in FIG.4; and for example, col.5, line 36 to col.9, line 25], and presents the digest data and the application electronic signature to the secure device, and wherein the secure device verifies the application electronic signature by using the presented digest data, and then authenticates the application if a verified result is normal [see col.9, line 25 to col.11, line 12].

Claim 9 is rejected for the same reasons applied to the rejection of Claim 2.

As per Claim 5, DeTreville-Barlow combination teaches,

an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking said application running means [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7], wherein said application running means is an application execution runtime environment [see FIGS.2 and 3],

wherein the application running means verifies an electronic signature of the application to which the electronic signature is attached to authenticate the application, and wherein the secure device accepts an authenticated result of the application running means to authenticate the application [see FIGS.14 and 15; and for example, col.23, line 14 to col.26, line 3].

As per Claim 6, DeTreville-Barlow combination teaches,

wherein the secure device l) shares a second information with the application running means if the secure device authenticates the application running means, and 2) accepts a process request if the second information are added to the process request issued from the application that the secure device authenticates [see FIGS.13-15].

As per Claim 10, DeTreville-Barlow combination teaches,

wherein the application runtime environment sends out the digest data to the secure device [see FIGS.2, 3 and 11], then acquires a collated result of the digest data from the secure device, and then authenticates the application [see FIG.5; **Equation 1** in col.9; and for example, col.5, line 35 to col.11, line 12].

Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over "DeTreville" in view of "Barlow", and further in view of Gould et al. (US 2002/00428979 A1, referred as "Gould")

As per Claim 3, DeTreville-Barlow combination teaches,

an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking said application running means [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7], wherein said application running means is an application execution runtime environment [see FIGS.2, 3 and 11]; and

wherein the application running means calculates digest data of the application and presents the digest data to the secure device, and wherein the secure device collates the presented digest data with digest data held in the database of the secure device, and then authenticates the application if a collated result is normal [see FIG.5; **Equation 1** in col.9; and for example, col.5, line 35 to col.11, line 12].

DeTreville discloses a database stored in the secure device [see **Data storage 129** in FIG.2]; but DeTreville-Barlow combination fails to disclose wherein the database includes predetermined digest data for authenticating a plurality of applications. However, Gould discloses the database includes predetermined digest data for authenticating a plurality of applications [see **Electronic Signature Database 22** in FIGS.1, 5 and 6].

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention was made, to modify the system of DeTreville-Barlow combination by incorporating Gould's teaching in order to authenticate users with signature card, which minimize unauthorized use [for example an identity theft; see abstract of **Gould**].

As per Claim 4, DeTreville-Barlow-Gould combination teaches,

wherein the application running means calculates digest data of the application and sends out a process request command to the secure device [see FIG.5; **Equation 1** in col.9; and for example, col.5, line 35 to col.11, line 12 of **DeTreville**], then wherein the secure device sends out first information to the

application running means, then wherein the application running means encrypts the first information by using the digest data and sends out encrypted information to the secure device, and then wherein the secure device decrypts the encrypted information by using the digest data stored in the database of said secure device and then collates decrypted information with the first information [see FIGS.14 and 15; and for example, col.23, line 14 to col.26, line 3 of **DeTreville**].

Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over "DeTreville" in view of "Lee" (US 7,000,249 B2)

As per Claim 12, DeTreville teaches,

A terminal [**Computer 118**], comprising: an application storage unit [see **Memory 112** and **Nonvolatile Memory 136** in FIGS.2 and 3] storing at least an application [see **Applications 124** and **S/W Program(s)** in FIGS.2, 3 and 11];

an application execution runtime environment verifying and executing said application [see FIGS.2, 3 and 11];

an Operating System (OS) [see **Operating System 160** in FIG.3] verifying and invoking said application execution environment [see **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7]; and

wherein the application execution runtime environment transmits data including a hash of said application to the secure device and the secure device verifies a validity of the hash of said application [see FIGS.4-6; and for example, col.7, line 32 to col.11, line 12].

DeTreville fails to disclose a Basic Input Output System (BIOS) verifying and invoking said OS; and a secure device verifying said BIOS. However, in the same field of endeavor, Lee teaches a BIOS verifying and invoking said OS and a secure device verifying said BIOS [see FIGS.1 and 5; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention was made, to modify the system of DeTreville to verify BIOS by secure device. The modification has a benefit of protecting public computers from attack and prevents computer systems from revealing private information that should be kept a secret [see col.1, line 22 to col.2, line 27 of **DeTreville**].

As per Claim 13, DeTreville teaches,

A method of verification of an application on a terminal [abstract], comprising the steps of: verifying and invoking an application execution runtime environment by the OS [see **Operating System 160** in FIG.3 and **Boot Block 162** in FIG.3 and **Ring A – Loader/Verifier 258** in FIG.7];

verifying an executing the application stored in an application storage unit of the terminal by the application execution runtime environment [see FIGS.2, 3 and 11]; and

transmitting data including a hash of said application to the secure device by the application execution runtime environment [see FIGS.14 and 15]; and verifying a validity of the received hash of the application by the secure device [see FIGS.4-6; and for example, col.7, line 32 to col.11, line 12].

DeTreville fails to teach verifying a Basic Input Output System (BIOS) by a secure device and verifying and invoking an Operating System (OS) by the BIOS. However, Lee teaches verifying a Basic Input Output System (BIOS) by a secure device [see FIGS.1 and 5; and for example, abstract] and verifying and invoking an Operating System (OS) by the BIOS [see FIGS.1, 3 and 4].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention was made, to modify the system of DeTreville to verify BIOS by secure device. The modification has a benefit of protecting public computers from attack and prevents computer systems from revealing private information that should be kept a secret [see col.1, line 22 to col.2, line 27 of **DeTreville**].

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139